UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/987,933	11/16/2001	Min-Ho Han	P67317US0	7908

43569 7590 01/11/2006

MAYER, BROWN, ROWE & MAW LLP
1909 K STREET, N.W.
WASHINGTON, DC 20006

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 01/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/987,933	HAN ET AL.	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 October 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Arguments

1. This communication is in response to applicants' response received on October 26, 2005.

2. Addition of claims 10 and 11 is acknowledged.

3. Applicant's arguments have been fully considered but they are not persuasive.

4. With regards to independent claims 1, 6 and 9, on page 6 of remarks, lines 17-29 applicants argue:

Malan does not relate to an intrusion detection or security since the networks that concern Malan are public; and

Malan does not teach or even suggest, tracking an intrusion based on the active packet transmitted to the intruder since Malan merely relies on information that was gathered about the originally transmitted packet. Therefore, both Malan and Comay fail to teach or suggest at least this feature of claim 1.

In response to above argument, Comay discloses a system and a method for automatic detection of an intruder source providing protection to a network (abstract and col. 2, lines 8-39). Malan discloses a method and system for protecting publicly accessible network computer services from undesirable sources (abstract, [0007] and [0008]). The services are normally residing on a private network that in this case publicly can be accessed.

Claim 1 recites that "...adding intrusion information associated with the intrusion into the packet, creating an active packet..." Comay discloses that the destination address of packet is changed back to the source address which corresponds to the recited adding intrusion information associated with the intrusion into the packet, because the source address belong to the unauthorized source. The packet with the new destination address is equivalent to the recited active packet. Malan on the other hand discloses a method that traces back an undesirable source (see, for example, [0091]-[0093]). Combining the teaching of Malan with the system of Comay would read on the limitations of claims 1, 6 and 9.

5. In light of the above submission the previous rejection of the original claims including the newly presented claims 10 and 11 is maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 5, 6, 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Comay et al (6,363,489 B1; hereinafter Comay) in view of Malan et al (2002/0035698 A1; hereinafter Malan).

Regarding claims 1, 6 and 9, Comay discloses:

A security system on a network, comprising (see Fig. 1): intrusion detecting means for detecting an intrusion through an analysis of a packet, adding intrusion information associated with the intrusion into the packet, creating an active packet and transmitting the active packet to an address of an intruder which transmitted the packet (see, for example, col. 2, lines 40-51; col. 5, lines 15-31; col. 5, lines 32-60, wherein changing the destination address to the source address corresponds to the recited adding intrusion information associated with the intrusion into the packet).

However, Comay does not expressly discloses routing means for tracking the intrusion, for all routes through which the intruder passed, based on the active packet transmitted thereto from the intrusion detecting means, and filtering the packet associated with the intruder, thereby isolating the intruder, wherein the routing means includes active nodes on a local networks of a user to be attacked and the intruder.

Malan teaches a system that protects a publicly accessible network services from undesirable network traffic in real-time (see, for example, Fig. 2; [0022]-[0027]). Malan teaches that the arriving packets are analyzed and filtered (see, for example, [0066] and [0072]). Malan further teaches a mechanism that backtrack the path that incoming packets have traveled through all the routers from the beginning to end to pinpoint the location of the intruder and filtering the packets from the attacker (see, for example, Figs. 6,10-15; [0091]-[0093]; [0096]; [0102]; [0109]). Malan also teaches that there are active routers on both protected network and the network of the intruder (see, for example, Fig. 10).

Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to implement a backtrack and filtering means as taught in Malan in the system of Comay to block an intruder at any layer or depth of a transaction and as close as possible to its original source (Malan, [0014] and [0098]).

Regarding claim 2, Malan discloses:

The system as recited in claim 1, wherein the intrusion detecting means includes

means for recognizing a local network from which the intrusion is originated, during the detection of the intrusion (see, for example, Fig. 8; [0055]; [0094]; [0107]); and

means for notifying the intrusion of a filtering means in a local network to which the user to be attacked belongs and that in a local network to which the intruder belongs (see, for example, [0053]; [0054]; [0072]; [0096]).

Regarding claim 3, Comay discloses:

The system as recited in claim 2, wherein the intrusion detecting means includes:

collection means for collecting packets which pass therethrough (see, for example; col. 4, lines 42-60, where the firewall at the entry point corresponds to the recited collection means);

analysis means for receiving the packet from the collecting means and determining whether the packet is one associated with intrusion or an active packet

(see, for example; col. 5, lines 15-30, where the intrusion detection module corresponds to the recited analysis means); and

processing means for processing the intrusion information or the active packet, which is received from the analysis means (see, for example; col. 5, lines 31-60, where the intrusion diversion module corresponds to the recited processing means).

Regarding claims 5 and 11, Comay discloses:

The system as recited in claims 1, wherein the routing means includes: filtering means for determining whether the packet is transmitted or not (see, for example, Fig. 2, step 3, wherein the scanning corresponds to the recited filtering);

classifying means for determining whether the packet from the filtering means is an active packet or an internet protocol (IP) packet, if the packet is the IP packet, forwarding the packet (see, for example, Fig. 2, steps 6, 7b and 8a, wherein the packet is forwarded if it is not associated with an intruder which corresponds the recited IP packet), and if the packet is the active packet, transmitting the packet to be executed at an active packet execution environment (see, for example, Fig. 2, steps 6, 7a and 8b, wherein the packet is determined that associated with an intruder which corresponds the recited active packet); and

means, if the packet classified by the classifying means is one associated with the intrusion information, for adding the packet information to be filtered to the filtering means and forwarding the packet through an IP forwarding engine (see, for example,

col. 6, lines 39-67 and Fig. 2, steps 6, 7a and 8b, wherein the packet information associated with an intruder is stored at the hostile DB).

Regarding claim 8, Comay discloses:

The method as recited in claim 6, wherein the step b) includes the steps of:

b1) classifying, if the packet inputted to the local network border router is one to be transmitted by filtering, whether the packet is an active packet or an Internet protocol (IP) packet (see, for example, Fig. 2, steps 6, 7a, 8b or 6, 7b and 8a, wherein the packets are determined associated with an intruder or not which corresponds the recited active or IP packet);

b2) if the packet is the IP packet, forwarding the packet (see, for example, Fig. 2, steps 6, 7b and 8a, wherein the packet is forwarded if it is not associated with an intruder which corresponds the recited IP packet); and

b3) if the packet is the active packet, determining, whether the packet is one associated with the intrusion information, and if so, storing the intrusion information and forwarding the packet (see, for example, col. 6, lines 39-67 and Fig. 2, steps 6, 7a and 8b, wherein the packet information associated with an intruder is stored at the hostile DB).

Allowable Subject Matter

Claims 4, 7 and 10 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abdulhakim Nobahar
Examiner
Art Unit 2132 A. N.

January 5, 2006

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100